(12) UK Patent Application (19) GB (11) 2 309 566 (13) A

(43) Date of A Publication 30.07.1997

(21) Application No 9601686.0

(22) Date of Filing 27.01.1996

(71) Applicant(s)
Ford Motor Company Limited

(Incorporated in the United Kingdom)

Eagle Way, BRENTWOOD, Essex, CM13 3BY, United Kingdom

(72) Inventor(s)
Duncan Bramley

(74) Agent and/or Address for Service
A Messulam & Co
24 Broadway, LEIGH-ON-SEA, Essex, SS9 1BN, United Kingdom

(51) INT CL^6
H04H 1/00 , G08G 1/0967

(52) UK CL (Edition O)
G4H HNMC HTG H1A H13D H14A H14D H14G H60
G4Q QAJ
U1S S1819

(56) Documents Cited
None

(58) Field of Search
UK CL (Edition O) **G4H HNMC HTG , G4Q QAJ**
INT CL^6 **G08G , H04H , H04L , H04N**
ONLINE:WPI

(54) Broadcast receiver

(57) A broadcast receiver has a decoder for receiving an encrypted broadcast signal that requires the payment of a subscription fee. The receiver comprises a processor, means 14 for storing a code specific to the receiver, manually operable switches 10 for enabling the user to enter an access code 12, and means 20 for receiving and decoding a broadcast time signal. The processor 16 is arranged to apply a cipher algorithm to the user entered access code 12 and the receiver specific code 14 to compute a time window 18, the decoder being enabled only when the broadcast time signal 20 falls within said time window 18 to permit reception of the encrypted broadcast signal.

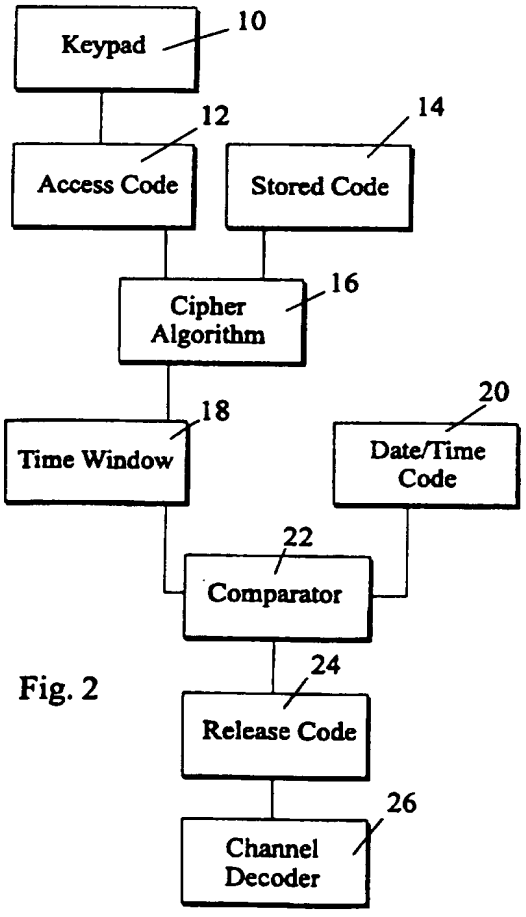

Fig. 2

GB 2 309 566 A

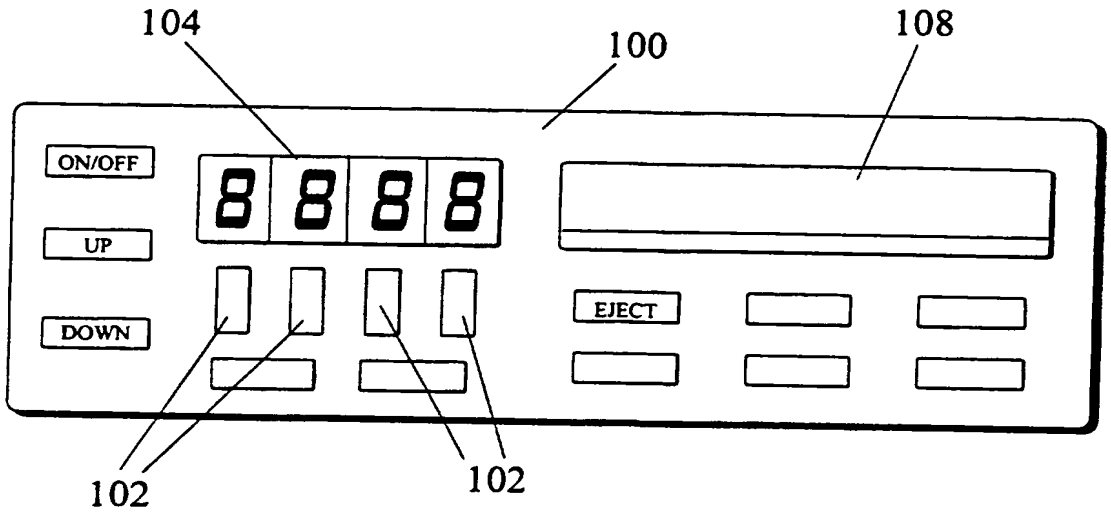

Fig. 1

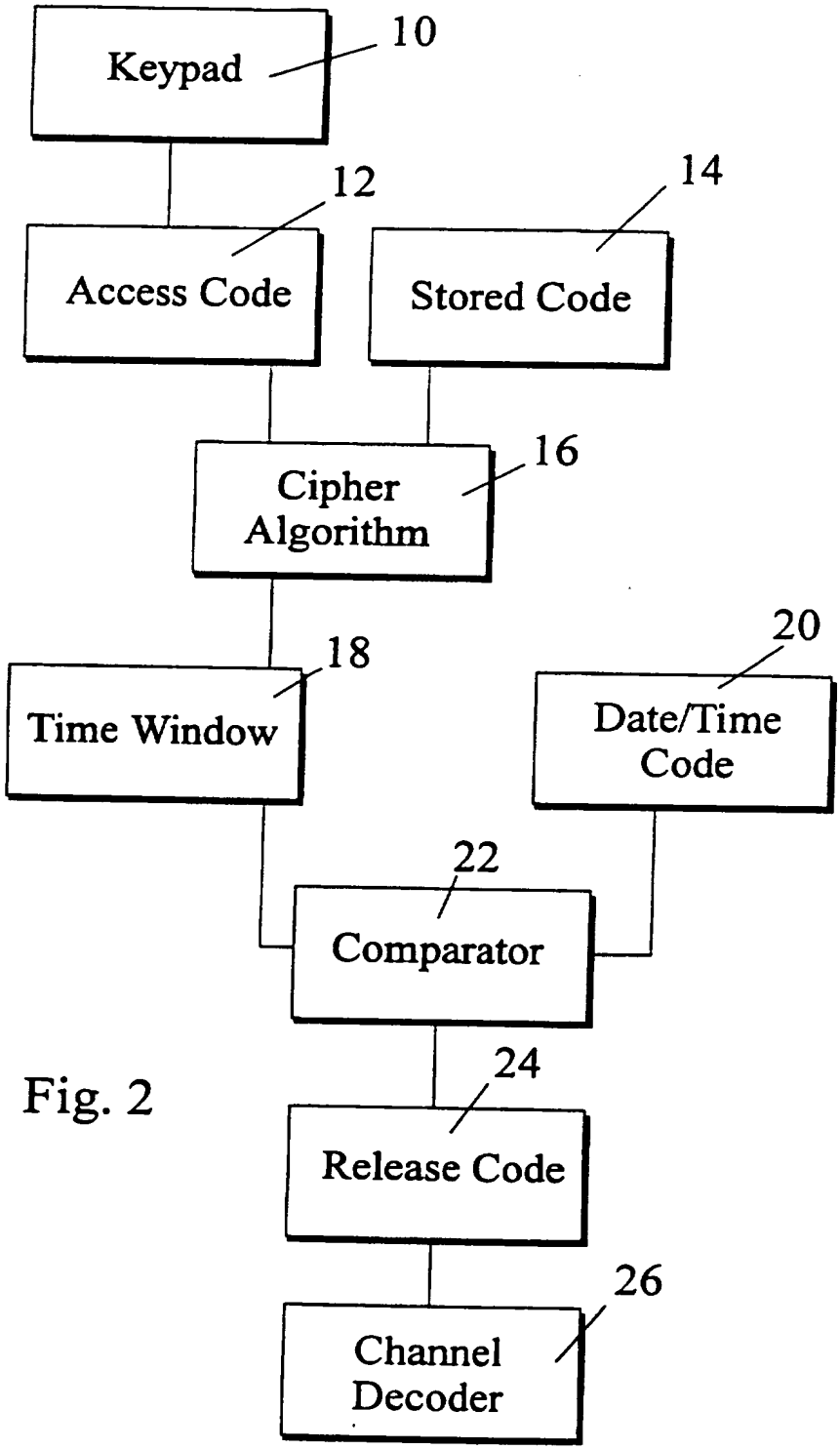

Fig. 2

BROADCAST RECEIVER

The present invention relates to a broadcast receiver for a motor vehicle and has particular application to a receiver having a decoder for receiving an encrypted broadcast signal that requires the payment of a subscription fee.

It is currently being proposed that traffic information should be made available to vehicle users on a dedicated channel that requires payment of a subscription fee.

In the case of satellite television channels to which subscription is necessary, current practice is for the broadcaster to supply the subscriber with an electronic key, in the form of an intelligent card, which it introduced into the broadcast receiver and permits decoding of the channel for the period of the subscription.

Within a vehicle, however, the use of such a card presents problems as space requirements make it difficult to incorporate a card reader within the radio receiver. Furthermore, such a card would exacerbate the common problem of theft of radio equipment from motor vehicles.

According to one aspect of the present invention, there is provided a broadcast receiver having a decoder for receiving an encrypted broadcast signal that requires the payment of a subscription fee, comprising a processor, means for storing a code specific to the receiver, manually operable switches for enabling the user to enter an access code, and means for receiving and decoding a broadcast time signal, wherein the processor is arranged to apply a cipher algorithm to the user entered access code and the receiver specific code to compute a time window, the decoder being enabled only when the broadcast time signal falls within said time window to permit reception of the encrypted broadcast signal.

To reduce the problem of theft of car radios, it is known for radios to require a key-code to be entered by the user after first installation. It would be possible in the same way to require all channel subscribers to enter a predetermined access code into the radio at the beginning of each subscription period to enable decoding of the encrypted channel during that period but such a system would be open to abuse if the same access code were needed by all radios.

The present invention avoids this problem by making the necessary access code specific to the receiver by combining the access code entered by the user with the stored receiver specific code, which could for example be the so-called key code or the stored serial number of the receiver. As a cipher algorithm is applied to the combination of the stored receiver specific code and the user entered access code, the access code will also be specific to each receiver.

If the cipher algorithm is maintained secret and is sufficiently complex, then it would be difficult to compute the correct access code. As with radio key codes, it can be made difficult for a user to attempt all possible code combinations by allowing only a limited number of attempts before the receiver is locked out for a prolonged period.

To subscribe to the service, the user would need to advise the service provider of the serial number of the broadcast receiver. The correct access code would then be computed and sent upon receipt of the subscription fee.

The cipher algorithm when applied to the combined access code and receiver specific code will compute a time window during which reception of the encrypted channel is permitted. As many broadcast channels contain a real time signal, the receiver can determine the real time and compare it with the computed time window to generate a signal for enabling or disabling the decoding of the encrypted channel.

It is preferred that the processor implementing the cipher algorithm should be the same processor as used to decode the encrypted broadcast channel so that there should not be an accessible connection between the two processors permitting the payment verification to be bypassed.

Alternatively, if two separate processors are used then an enabling code should be passed from one processor to the other to enable decoding of the encrypted broadcast.

The invention allows the same hardware as currently present in vehicle radios to be used to allow reception of encrypted channels but only by subscribers. The payment verification is secure and cannot readily be bypassed.

Furthermore, the invention offers additional security to the vehicle owner in that a stolen radio can only be made to receive encrypted channels by notifying the service provider of the serial number of the radio, thereby allowing it to be traced. A radio with the facility to receive encrypted channels would therefore have little value if stolen. This is to be contrasted with a radio containing a subscription card, where the stolen radio will operate correctly when reinstalled in another vehicle and where the subscription card would itself be an item prone to theft, as it can be used in any receiver.

The principle of the invention can also be used to provide an additional safeguard against theft for any vehicle receiver, even if it is not fitted with a decoder for an encrypted channel.

Thus, in accordance with a second aspect of the invention, there is provided a broadcast receiver comprising a processor, means for storing a code specific to the receiver, manually operable switches for enabling the user

to enter an access code, and means for receiving and decoding a broadcast time signal, wherein the processor is arranged to apply a cipher algorithm to the user entered access code and the receiver specific code to compute a time window, normal operation of the receiver being enabled only when the broadcast time signal falls within said time window.

In this aspect, the invention would require a new access code to be entered at regular intervals into the receiver. If the access code is only sent by radio manufacturer by mail to the registered owner of the receiver, the whereabouts of the receiver can always be traced and any stolen radio would be of little value because even if its key code and current access code are known, the whereabouts of the receiver would have to be revealed to the manufacturer at the end of the period set by the current access code to permit its continued use.

The invention will now be described further, by way of example, with reference to the accompanying drawings, in which:

Figure 1 shows the front panel of a car radio and cassette player, and

Figure 2 is a diagram showing the principle of operation of the invention.

The hardware for the implementation of the present invention need not differ from a conventional radio requiring a key code to safeguard against theft. The front panel of a typical such receiver and cassette player 100 is shown in Figure 1 of the drawings. The receiver has a slot 108 for receiving a magnetic audio cassette, a variety of switches beneath the cassette for the normal functions such as FORWARD, REVERSE, PLAY, SKIP, EJECT and so on. To the left of the cassette slot 108, a digital display 104 is mounted

on the front panel which can display the time, the frequency or identification of the selected channel and other data. To the left of the display 104 there are switches for switching the receiver on and off and UP/DOWN switches for setting, the volume, the tone, the channel, balance etc. Lastly, beneath the display, there are four preset channel selection switches 102 and mode selection switches. As the receiver is conventional, it is not deemed necessary to describe all its functions in detail.

If the receiver has a key code, then when it is first connected to a power supply, the display 104 displays horizontal lines or a message to indicate that it awaits entry of a key code. A key code is entered using any of the numerous switches provided on the front panel. For example each of the switches 102 normally used for selecting preset channels, can correspond to one of the digits of the key code and can be used to increment one of the code digits with each depression until the desired code is displayed. When a further button is depressed to indicate the end of code entry, the entered code is compared with that stored in the receiver and the amplifier and tuner are then enabled when the codes match. Three attempts are allowed to enter the correct code and thereafter the radio must be switched off and left for a prolonged period of time before another attempt at entering the key code is allowed. This is a safeguard against someone trying to discover the correct key code by trial and error.

Referring now to Figure 2, in order to allow reception of an encrypted channel, the present invention requires an access code to be entered into the receiver using a combination of the various switches on the front panel, which can be regarded as a keypad 10. The access code is entered into a register 12 and is combined with a code permanently stored in a read only memory 14. A processor 16 applies a cipher algorithm to the combined access code and stored code to

create a signal corresponding to a time window. For example, when the cipher algorithm is applied to the combined codes, it may generate the year (e.g. 1996) for which the licence fee has been paid. If the licence is not renewal annually, then the code stored in the time window may be the date of commencement and the duration of the licence.

Many broadcast channels include a time signal from which the current time and date can be recorded. Data decoded from such a channel is stored in a register 20 and compared by a comparator 22 with the time window for which the licence fee has been paid. If the comparator 22 determines that the current date falls within the licensed period, then it generates in a block 24 a release code that is applied to enable full operation of the channel decoder 26 for the encrypted channel.

The access code required to permit reception of the encrypted channel will vary with the stored code within the receiver, which could be the key code or the serial number of the receiver. Thus, each user will require a unique access code to permit reception of the encrypted channel. This code would be given to the user upon registration for the service, which could be for example a channel carrying traffic information. The user would notify the service provider of the stored code, which would already be known to him, and would be given the corresponding access code required to enable reception of the service. Provided that a secret cipher algorithm of sufficient complexity is used, it would not be a simple matter to compute the access code from known stored codes and the payment verification system would be sufficiently secure.

The invention offers the advantage that no special hardware, such a card reader, is required to determine if a licence fee has been paid. Furthermore, instead of offering an

additional incentive to would be car thieves, the invention detracts from the value of a stolen radio receiver in that the facility to decode the encrypted channel can only be used by revealing the whereabouts of the receiver to the service provider.

This principle can be extended to offer additional protection for any car radio by requiring an access code to be entered at regular intervals rather than just during initial installation. In this case, the access code would not in this case be used to enable the decoder of the encrypted channel to operate but to enable the entire receiver to operate. Therefore, the key code and the access code would be needed to allow a newly installed receiver to operate and thereafter a new access code would need to be entered periodically to allow continued operation of the receiver.

CLAIMS

1. A broadcast receiver having a decoder for receiving an encrypted broadcast signal that requires the payment of a subscription fee, comprising a processor, means for storing a code specific to the receiver, manually operable switches for enabling the user to enter an access code, and means for receiving and decoding a broadcast time signal, wherein the processor is arranged to apply a cipher algorithm to the user entered access code and the receiver specific code to compute a time window, the decoder being enabled only when the broadcast time signal falls within said time window to permit reception of the encrypted broadcast signal.

2. A receiver as claimed in claim 1, wherein the processor implementing the cipher algorithm is the same processor as used to decode the encrypted broadcast channel.

3. A broadcast receiver comprising a processor, means for storing a code specific to the receiver, manually operable switches for enabling the user to enter an access code, and means for receiving and decoding a broadcast time signal, wherein the processor is arranged to apply a cipher algorithm to the user entered access code and the receiver specific code to compute a time window, normal operation of the receiver being enabled only when the broadcast time signal falls within said time window.

3. A broadcast receiver constructed, arranged and adapted to operate substantially as herein described with reference to and as illustrated in the accompanying drawings.

Patents Act 1977 **Examiner's report to the Comptroller under Section 17 (The Search report)**	Application number GB 9601686.0
Relevant Technical Fields (i) UK Cl (Ed.O) G4H (HTG, HNMC), G4Q (QAJ) (ii) Int Cl (Ed.6) H04H, G08G, H04L, H04N	Search Examiner M J DAVIS Date of completion of Search 22 FEBRUARY 1996
Databases (see below) (i) UK Patent Office collections of GB, EP, WO and US patent specifications. (ii) ONLINE: WPI	Documents considered relevant following a search in respect of Claims :- 1-4

Categories of documents

X: Document indicating lack of novelty or of inventive step.

Y: Document indicating lack of inventive step if combined with one or more other documents of the same category.

A: Document indicating technological background and/or state of the art.

P: Document published on or after the declared priority date but before the filing date of the present application.

E: Patent document published on or after, but with priority date earlier than, the filing date of the present application.

&: Member of the same patent family; corresponding document.

Category	Identity of document and relevant passages	Relevant to claim(s)
	NONE	

Databases: The UK Patent Office database comprises classified collections of GB, EP, WO and US patent specifications as outlined periodically in the Official Journal (Patents). The on-line databases considered for search are also listed periodically in the Official Journal (Patents).

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.